나무위키

Tails OS/사용 방법

최근 수정 시각: 2026-07-14 22:24:20

분류:Debian | 컴퓨터 보안 | 프라이버시

상위 문서: Tails OS

목차

1. 개요
2. 하드웨어 호환성 문제
3. 부트 미디어용 저장장치 선택하기
4. 설치/사용법 간단 가이드
5. 시작 화면(Welcome Screen)
6. Persistent Storage 이용
   6.1. 추가 저장장치 이용하기
7. Windows/macOS와 병용
8. 인터넷 이용
   8.1. Tor 브릿지 접속 불가 문제 해결
   8.2. 무선 인터넷 연결 문제 해결
9. 익명으로 회원가입하기
   9.1. 이메일 인증이 불필요한 경우
   9.2. 이메일 인증이 필요한 경우
10. 비트토렌트 사용?
11. Tails 업그레이드
12. 사용 종료 직후 해야 할 일
13. Tails 부트 미디어 초기화

1. 개요

정확한 최신 정보는 공식 홈페이지에서 확인하는 것이 바람직하나, 공식 홈페이지는 한국어를 지원하지 않으므로 영어를 잘 하지 못한다면 이 항목을 참조하는 것도 방법이다.

이 문단은 2023년 12월 많은 내용이 개정됐다. 이전 내용이 필요하다면 r175 리비전을 참조하면 된다.

2. 하드웨어 호환성 문제

Tails 공식 홈페이지 알려진 문제 페이지
Tails 공식 홈페이지 알려진 그래픽 카드 문제 페이지
Tails 공식 홈페이지 부팅 옵션 수정 페이지

데스크톱 컴퓨터는 너무 오래되지 않았고 AMD 그래픽 카드를 사용하지 않는다면[1] Tails 구동에 아무 문제가 없는 경우가 대부분이다.

랩톱 컴퓨터는 크기를 작게 하기 위해 다양한 부품을 사용하기에 이에 맞는 대응[2]이 되어 있지 않은 경우가 데스크톱보다 훨씬 많기 때문에 부팅이 안 되거나, 부팅은 되는데 키보드가 작동하지 않거나 Wi-Fi 접속이 안 되거나 소리가 안 나오거나 하는 경우가 있다. 부팅이 안 되거나 소리가 안 되는 경우에는 마땅한 해결책이 없다.

공식 홈페이지에서는 Intel CPU 내장 그래픽 하드웨어를 사용하고, NVIDIA/AMD 제품을 피할 것을 권장하고 있다. 부팅 옵션을 수정하면 부팅이 되는 경우도 있다. 이 경우 시작 전 매번 부팅 옵션 수정 작업이 필요하므로 이용이 불편하다.

기본 옵션으로 Tails 부팅이 안 되는 몇 가지 사례를 적어둔다.

1. AMD Radeon HD 시리즈, R9 290/390, RX 480, RX Vega - 부팅 옵션 수정이 필요하다.
2. Dell Latitude E5250/E6230/E6430 - 부트 미디어로 부팅이 불가능하다.
3. Dell XPS 15 7590 - NVIDIA 그래픽 카드 장착 모델은 원활한 부팅을 위하여 부팅 옵션 수정이 필요하다.
4. MacBook Pro 및 MacBook Air 2018 이후 모델 - 부팅 옵션 수정이 필요하며, 내장 키보드와 트랙패드를 사용할 수 없다. Apple T2는 기본적으로 외부 OS에서의 내장 장치를 차단하기 때문인다. 외부 장치를 연결하여 사용은 가능하다.
5. Microsoft Surface Laptop 3/4 - 부팅은 가능하나, 키보드와 마우스를 사용할 수 없다. 외부 장치도 포함된다. MacBook Air Retina와 달리 부팅 옵션 수정으로 해결할 수 없으므로 이 문단에 적어둔다.

부팅은 되나 정상 구동이 안 되는 경우도 있다. 몇 가지 사례를 적어둔다.

1. 다중 그래픽 하드웨어 - 화면이 검게 표시될 수 있다. BIOS/UEFI 설정에서 사용할 그래픽 하드웨어를 명시적으로 설정하거나, 부팅 옵션 수정이 필요하다.
   NVIDIA Optimus와 같이 그래픽 하드웨어 전환 기능이 있는 경우 이 문제가 발생할 수 있다. MacBook Pro Mid 2010/Early 2011/Early 2013 Retina에서 이 문제가 보고됐다.
2. 터치패드 미작동 - Acer C720/Lenovo IdeaPad 3에서 보고됐다. 부팅 옵션 수정으로 해결할 수 있다.
3. Lenovo Legion Y530 - 무선 랜이 작동하지 않는다. 부팅 옵션 수정으로 해결할 수 있다.
4. Lenovo ThinkPad 11e - 일부 모델에서 불안정 작동이 보고됐다. 부팅 옵션 수정으로 해결할 수 있다.
5. Radeon R9을 사용하는 MacBook - Tor 브라우저와 ThunderBird에서 그래픽 오류가 보고됐다. 부팅 옵션 수정으로 해결할 수 있다.
6. 88W8897 - 내장 무선 랜 카드이다. 일부 컴퓨터에서 Wi-Fi 연결이 안 될 수 있다.
7. RTL8821CE - 내장 무선 랜 카드이다. Linux에서 사용할 수 없는 하드웨어이다.
8. RTL8723BE - PCIe 무선 랜 카드이다. Wi-Fi 연결이 되지 않거나 성능이 저하될 수 있다. 제시된 여러 부팅 옵션 중 자신에게 맞는 값을 찾아 적용해야 한다.
9. 일부 Broadcom 무선 랜 카드 - 드라이버 소프트웨어 설치가 필요하다. 사유 소프트웨어이므로 Tails에 포함되지 않는다.
10. GIGABYTE 메인보드 - USB 인식이 안 될 수 있다. USB 2.0 포트를 사용하거나, BIOS/UEFI 설정을 조정하거나, 부팅 옵션을 수정하는 방법이 제시되어 있다. 이러한 방법을 사용할 경우 일부 USB 포트가 비활성화될 수 있다는 점에 유의하여야 한다.

이는 보고된 사례일 뿐이며, 보고되지 않은 문제가 언제든 발생할 수 있다.

보안 문제로 Bluetooth 사용은 불가능하다.
USB 무선 랜 카드는 Panda Wireless Ultra, Panda Wireless PAU05, ThinkPenguin TPE-N150USB(Qualcomm Atheros AR9271)가 공식적으로 호환된다고 밝혔다. Tails 5.19.1에서 Realtek RTL8192FM을 사용하는 nexi NX-300N 인식이 가능했다.

하드웨어 호환성과 관련하여, Tails 5는 Debian 11 기반으로 만들어졌음을 참고할 수 있다.

3. 부트 미디어용 저장장치 선택하기

Tails 이용을 위해서는 이동식 저장장치가 필요하다. 보통 USB 플래시 드라이브를 사용한다.
최소 용량인 8 GB 이상이기만 하면 용량이 크게 중요하지는 않다. 용량이 크면 그만큼 안에 더 많은 파일을 저장할 수 있을 테지만, 용량이 작더라도 다른 저장장치에 따로 보관하면 된다. 다만 이렇게 사용할 경우에는 Tails 부트 미디어와 다른 저장장치, 총 2개를 컴퓨터에 연결해야 하므로 약간 귀찮아지기는 한다. 보안은 약간 떨어지지만, 편의를 위해서는 공간이 넉넉한 저장장치 하나로 해결하는 것이 낫다. 2023년 12월 현재 128 GB USB 플래시 드라이브는 송료 포함 1.5만 원 내외이고, 일부 다이소 매장에서는 Sandisk Cruzer Blade 32 GB 제품을 5천 원에 판매한다.

만약 Tails 부트 미디어 자체에 파일을 저장할 계획이라면, 16 GB 이상이면서 USB 3.0 이상을 지원하는 제품을 권한다. 부팅 파티션이 8 GB를 사용하니 최소 16 GB가 필요하고, Tails는 USB 2.0 대역폭으로도 무리 없이 동작하나 파일 입출력용으로는 부족하다. 쉽게 말해 속도가 많이 느리다.

4. 설치/사용법 간단 가이드

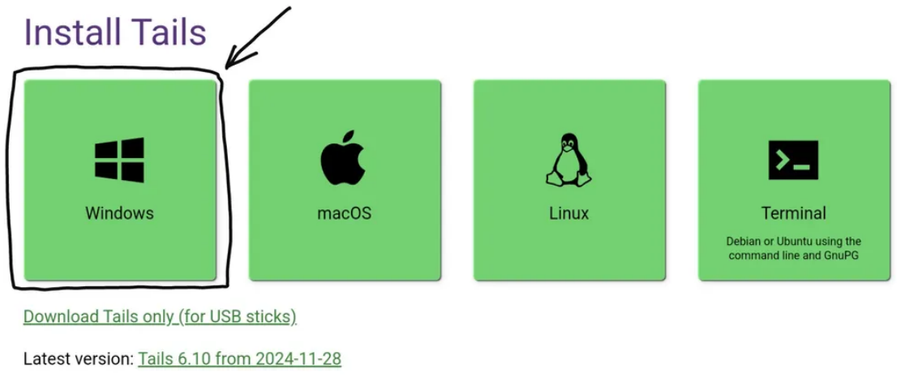
주의: 이 가이드는 오래됐으며, 틀린 내용이 있을 수 있다. 교차검증이 바람직하다.

Tails OS의 설치 방법을 간단히 설명하자면,

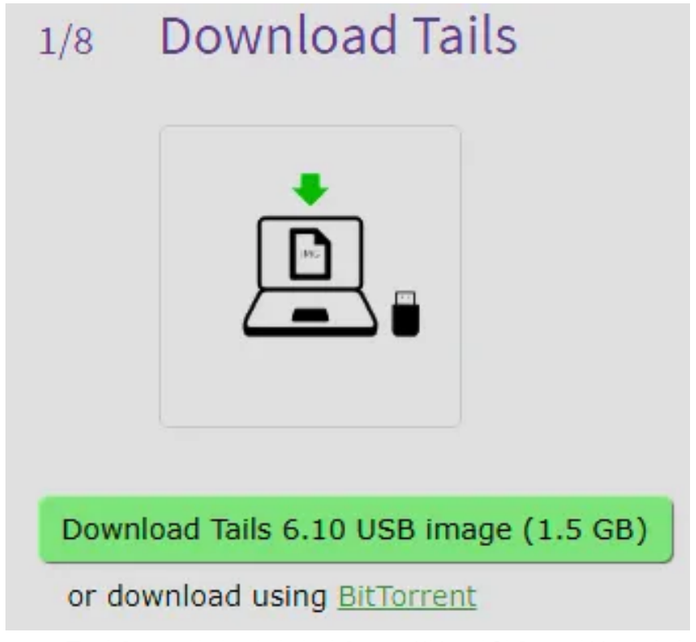
0. 용량이 최소 8 GB 이상인 이동식 저장장치를 준비한다. 주로 USB 플래시 드라이브를 많이 사용하며, 영구 스토리지를 사용할 경우 16 GB 이상을 권장한다.
1. Tails OS 파일을 다운받는다.
2. Rufus를 다운 받는다.
3. Rufus를 이용해 Tails 부트 미디어를 제작한다.
4. 컴퓨터를 재시작하여 제작한 부트 미디어로 부팅한다. BIOS/UEFI의 부팅 순서를 바꾸어야 한다. Windows 설치를 해 보았다면 이해가 쉬울 것이다.
5. Tails로 부팅이 되면 우측 상단 Start Tails를 클릭하여 Tails를 이용한다.

🔗 이미지로 보는 Tails OS 설치 방법

0. Tails 부트 미디어 제작하기
1. Tails 웹사이트에 접속한다. 🔗 클릭하여 Install Tails 페이지로 바로 이동
2. 대부분 Windows를 사용할 것이므로, Windows 클릭 🔗 참고 1 🔗 참고 2

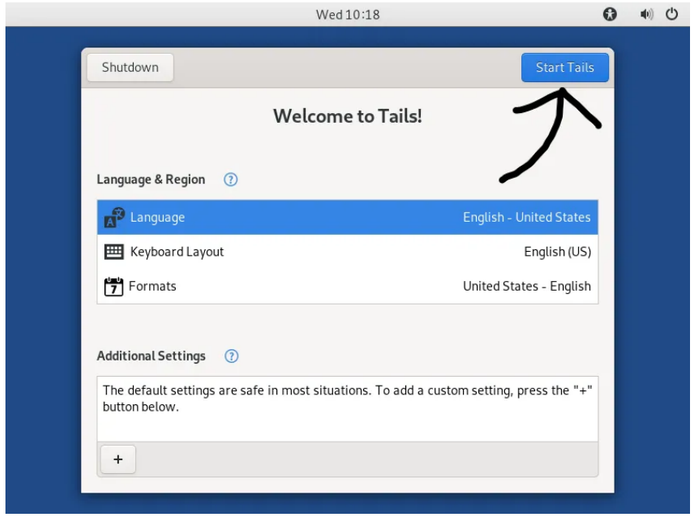


3. Tails 설치용 이미지를 다운로드한다.

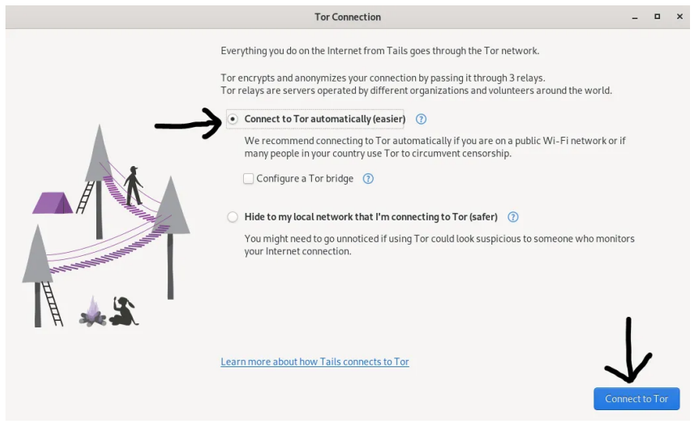


4. Rufus를 다운로드한다. 여기서 다운로드 받는 파일은 포터블 버전이다.
5. Rufus를 이용하여 부트 미디어를 제작한다. 구동을 위해 약 350 MB의 디스크 여유 공간이 필요하다.
   다른 도구 사용은 권장되지 않는다.
   Tails FAQ [펼치기 · 접기]

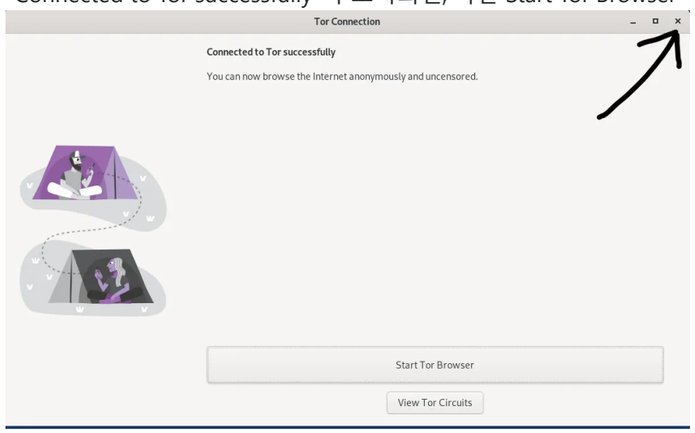
0. Tails로 부팅하고 Tor 브라우저 사용/한글 입력 설정하기
1. 컴퓨터를 재시작하고 제작한 부트 미디어로 부팅한다. BIOS/UEFI에서 부팅 순서 변경을 해야 한다. Windows 설치를 해 보았다면 이 작업은 쉬울 것이다. 🔗 참고 링크
2. 우측 상단 Start Tails 버튼 클릭



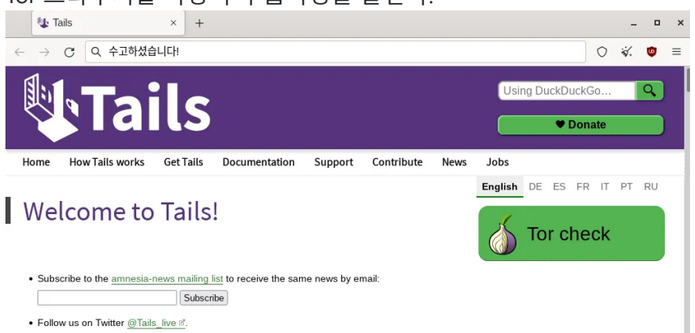
3. 네트워크에 연결되어 있다면 Tor connection 창이 뜬다. Connect to Tor automatically (easier)를 선택한 상태에서 Connect to Tor 클릭.



4. "Connected to Tor successfully"가 표시되면, 하단 Start Tor Browser 버튼을 눌러 Tor 브라우저를 실행할 수 있다.

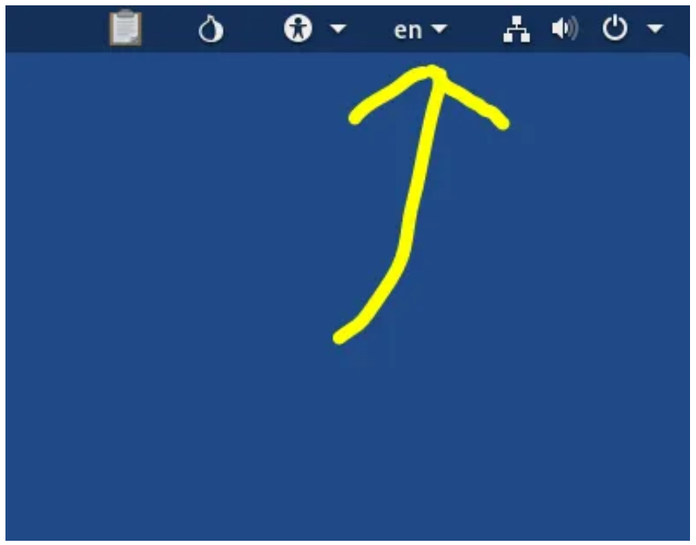


5. Tor 브라우저를 사용하여 웹서핑을 즐긴다.

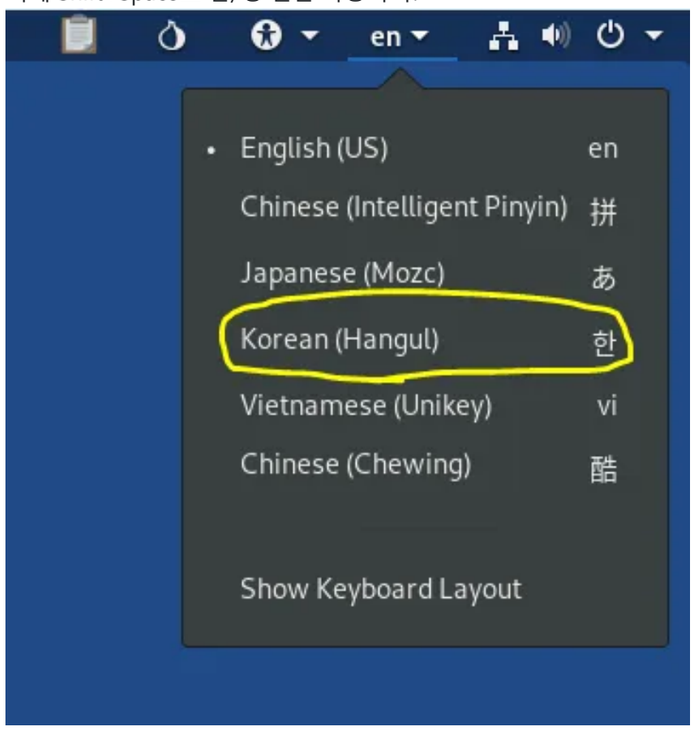


이제 한글 입력을 설정해 보자.

6. 화살표로 표시한 아이콘 클릭



7. Korean(Hangul) 선택.
이제 Shift+Space로 한/영 전환 가능하다.



Shift+Space가 불편하다면 처음에 누른 화살표로 표시한 아이콘 선택 - Setup 으로 IBusHangul Setup 창을 연 후, Hangul Toggle Key 설정을 해 주면 된다. Add를 누르고 원하는 키를 누르고 OK, 우측 하단 OK를 누르면 원하는 키를 한/영 키로 설정할 수 있다.

'Tails 설치' 등의 키워드로 검색하여 나오는 자료를 참조하는 것도 방법이다.

5. 시작 화면(Welcome Screen)

Tails 공식 홈페이지 Welcome Screen 페이지
Tails로 부팅하면 Welcome to Tails!라면서 이것저것 설정하는 창이 뜬다. Language & Region을 제외한 설정은 지금

해야 한다. 보안상 이유로 Tails를 시작한 후에는 설정을 바꿀 수 없다. 설정을 바꾸려면 재부팅을 해서 Welcome Screen에 다시 접근해야 한다.

1. Language & Region
Language - 말 그대로 언어이다. Tails는 여러 언어를 지원하며 한국어도 지원한다.
Keyboard Layout - 키보드 배열을 설정하는 항목이다. 키보드별 한/영 키 처리 차이 문제로, 초보자는 불편하더라도 이 설정을 기본값인 English로 두고 #한글 입력기 설정 방법 문단을 따라하는 것을 권한다. Korean과 Korean(101/104-key compatible)의 차이를 알 정도 지식이 있다면 적절한 설정 값을 변경하여도 무방하다.
Formats - 날짜 표기 등을 어떻게 할지를 선택하는 항목이다. 기본값으로 두는 것을 권한다.

2. Persistent Storage
아직 만들지 않았다면 "Create Persistent Storage" 버튼이, 만들었다면 비밀번호 입력 창이 뜰 것이다. 말 그대로 비밀번호를 입력하면 된다.
비밀번호를 입력하지 않아도 Tails를 시작할 수 있으나, Persistent Storage에 있는 데이터에 접근할 수 없다.

3. Additional Settings
관리자 비밀번호 활성화, 랜덤 MAC 비활성화, 오프라인 모드 활성화, Unsafe Browser 비활성화와 같은 추가 설정을 할 수 있다. 오프라인 모드와 Unsafe Browser 비활성화를 제외한 모든 설정은 보안을 약화시키며, 오프라인 모드는 실행하면 당연하게도 인터넷에 연결할 수 없다.

1. 관리자 비밀번호는 내장 저장장치 마운트, 소프트웨어 설치, 터미널 sudo 권한 등에 사용된다.
2. 랜덤 MAC 비활성화는 익명성 확보 면에서 권장되지 않으나, MAC 주소로 인증하는 네트워크에 접속할 경우를 위해 존재하는 기능이다. 무선 랜 카드와 호환성 문제가 있는 경우 네트워크 접속을 위해 이 옵션을 활성화해야 할 수도 있다.
3. 오프라인 모드 활성화는 모든 네트워크 연결을 차단한다.
4. Unsafe Browser는 Tails 내에서 유일하게 Tor가 아닌 네트워크로 통신한다. Tails 공식 홈페이지에서는 Unsafe Browser를 공공 네트워크[3] 접속과 신뢰할 수 있는 내부 네트워크 접근 등 제한적 목적으로만 사용할 것을 권장한다. Tails 5.8부터 Unsafe Browser가 기본적으로 활성화되도록 바뀌었다.

특별한 이유가 없다면, 이 설정이 무엇을 의미하는지 모른다면 이쪽 설정은 기본값으로 두는 것이 바람직하다.

6. Persistent Storage 이용

Tails 공식 홈페이지 Persistent Storage 페이지

1. 이제 Persistent Storage를 활성화할 차례다. Persistent Storage는 Tails 부트 미디어에 구성되는 파티션이다. 부트 미디어에 Tails용 파일을 담고 남는 공간에 데이터 파티션을 하나 만들어 둔 것으로 이해하면 된다.

2. Tails는 보안을 중시하기 때문에 컴퓨터를 종료할 경우 저장된 모든 자료가 삭제된다. 하지만 Persistent Storage에 저장된 자료는 그 이름(영구 스토리지)답게 영구히 남게 된다. 공격자는 Persistent Storage의 존재를 알 수 있다는 점에 유의하여야 한다. 보안 수준 하락을 감안하더라도 Tails 부트 미디어에 파일을 저장해야겠거나 설정 값 유지가 필요하다면 문단을 계속 읽으며 Persistent Storage 구성을 진행하면 된다. 단순한 자료 저장만 필요하다면 저장장치를 하나 더 사용하는 것을 권한다. 이 문단을 닫고 바로 밑 문단을 열어 그 내용대로 진행하자.

3. Tails 부팅 후, 좌측 상단 Applications → Tails → Configure Persistent Storage을 누른다. 그러면 비밀번호를 정하는 창이 뜬다. 앞으로 Persistent Storage 안에 저장되는 데이터는 그 비밀번호로 암호화된다. 비밀번호를 모르는 공격자는 데이터를 볼 수 없지만, 비밀번호를 아는 공격자는 (당연하게도) 데이터를 볼 수 있다.

4. 비밀번호는 지금까지 쓰던 것 말고 새롭게 만드는 것이 좋다. 평소에 쓰던 비밀번호는 이미 가족, 친구 등이 (어떤 경로로든) 알고 있을 가능성이 높기 때문이다. 또한 당연하게도, 비밀번호는 강력해야 한다. 1q2w3e4r 같은 것은 영좋지 않다.

기억하기도 쉽고 입력하기도 쉬우면서도 강력한 비밀번호를 어떻게 만들어야 하는지가 문제된다. 일반적으로, 기억 및 입력의 편의성과 비밀번호의 강력함은 서로 대척되는 관계에 있다. 1Qaz2Wsx!은 기억하기도 쉽고 입력하기도 쉽지만, 강력하지는 않다. (대문자, 소문자, 숫자, 특수문자가 모두 포함된 8자리 이상의 비밀번호라고 해서 반드시 강력한 것은 아니다!) 반대로 R:mU8uE2z1w.|HFr=y5{lrT/CS4h)A은 강력하지만, 기억하기도 어렵고 입력하기도 어렵다.

5. 이러한 딜레마를 해결하는 방법이 있다. 서로 관련 없어 보이는 '단어' 6개 이상을 골라 아무렇게나 배열함으로써 비밀번호를 만드는 것이다. 예를 들어 '종교사회학 광고주 갈매기 도미니카 공소시효 까막눈'을 통째로 비밀번호로 사용한다고 생각해 보자(비밀번호에 띄어쓰기를 포함해도 된다. 프로그램은 띄어쓰기도 하나의 문자로 인식한다). 기억하기도 쉽고 입력하기도 쉬우면서도 나름대로 강력하다. 단어를 선택할 땐 되도록이면 단어들 간에 서로 관련 없는, 그리고 나 자신과도 관련 없는 단어를 선택하는 것이 좋다. 예를 들어 '김영삼 김대중 노무현 이명박 박근혜 문재인'은 명목상으로는 6단어로 된 비밀번호이지만, 실질적으로는 랜덤하게 고른 6개의 단어에 비해 추측해 내기가 훨씬 쉬울 것임을 알 수 있다. 자기의 생년월일이나 출신학교나 출신동네 이름을 넣는다거나, 자기가 소중히 여기는 사람이나 동물이나 가치관의 이름을 넣는다거나, 자신의 직업상 자주 접하게 되는 개념 또는 사람의 이름을 넣는다거나 하는 것도 비밀번호의 추측가능성을 증대시키는 요인이 된다. 최대한 랜덤해 보이게 만드는 것이 좋다.

단어 여럿을 사용하는 것은 Tails 측에서도 권장하는 방법이다. r175 리비전에는 KeePassX를 사용하여 랜덤 비밀번호를 만드는 방법을 제시했으나, 암기가 쉽지 않으므로 이 방법은 삭제했다. 종이에 적어 두어 암기하라는 내용도 보안상 문제가 있으므로 삭제했다.

이제 그렇게 정한 비밀번호를 Persistent Storage의 비밀번호로 삼는다. 이 비밀번호는 오직 Tails에만 사용하고, 다른 곳에는 사용하지 않는 것을 권장한다.

6. 비밀번호를 설정하고 확인 버튼을 누르면, 'Specify the files that will be saved in the persistent volume'이라면서 Personal Data, GnuPG, SSH Client 등 다양한 것을 설정할 수 있는 창이 뜬다. 이 설정은 어차피 나중에 바꿀 수 있으니 지금은 크게 고민하지 않아도 된다. 하나하나 읽어보고 필요한 것에만 체크하는 것이 낫다. 일단은 Personal Data에만 체크하는 것을 추천한다. 브라우저 즐겨찾기 기능을 사용한다면 Browser Bookmarks, 무선 네트워크를 사용한다면 Network Connections도 체크하여야 한다. (체크 안 하면 매번 Wi-Fi 비밀번호를 입력하여야 한다)

6.1. 추가 저장장치 이용하기

Tails 공식 홈페이지 LUKS 암호화 볼륨 설정 페이지
Tails 부트 미디어에 Persistent Strage를 세팅하면 그 안에 설정 값, 파일 등을 저장할 수 있다. 하지만 공격자는 Persistent Stoarge의 존재를 알 수 있으므로, 보안 상 다른 저장장치를 준비하여 그 안에 자료를 담는 것을 권한다. 이 저장장치는 파티션 암호화가 되어 있어야 하며, 사용이 끝난 후에 잘 숨겨야 한다.

Tails로 부팅된 상태에서 다른 이동식 저장장치를 연결하면 자동으로 인식한다. Windows와 똑같다. 그러나 파티션 암호화가 되어 있지 않다면, 그 파일은 당연하게도 암호화되지 않은 상태로 저장된다. 공격자는 그 저장장치를 자기 컴퓨터에 연결하기만 하면 안에 든 파일을 다 열어볼 수 있다.

따라서 외부 저장장치에 파일을 보관하고자 하는 경우에는 먼저 파티션 암호화부터 해 놓아야 한다. 구체적인 방법은 다음과 같다.

0. 기존에 들어있던 파일 중 보관할 가치가 있는 것들을 다른 저장장치로 옮긴다. **저장된 모든 데이터가 삭제**되기 때문에, 필요하다면 반드시 데이터 이동 작업을 해야 한다.
1. Tails로 부팅하고, 외부 저장장치를 연결한다.
2. Applications → Utilities → Disks로 들어가 왼쪽에 있는 디바이스 목록에서 그 저장장치에 해당하는 디바이스를 선택한다. 디바이스 이름(제조사와 모델명이 표시될 것이다), 용량 등을 보고 판단하면 된다.
3. 우측 상단에 가로줄 3개 모양 아이콘을 눌러서 Format Disk를 선택한다. 위에 거는 Don't overwrite existing data (Quick), 아래 거는 Compatible with modern systems and hard disks > 2TB (GPT)를 선택한다.

4. 이제 창 중간쯤에 있는 + 모양 아이콘을 누른다. 그러면 Create Partition이라는 창이 뜨는데, Erase는 'Don't overwrite existing data (Quick)', Type은 'Encrypted, compatible with Linux systems (LUKS + Ext4)', Name은 그 저장장치의 이름으로 삼고 싶은 단어 아무거나 입력, Passphrase는 그 저장장치를 암호화할 비밀번호(Persistent Storage를 만들었다면, 여기서 썼던 비밀번호와 다른 비밀번호로 설정하는 것을 추천한다)를 입력한다. 이 비밀번호를 아는 사람은 그 저장장치의 내용을 쉽게 들여다볼 수 있다는 점에 유의하여야 한다.
5. 모든 끝났으면 이제 그 저장장치에 자유롭게 파일을 넣으면 된다. Tails로 부팅한 상태에서 그 저장장치를 꽂으면 비밀번호를 입력하라는 창이 뜰 것이다. 거기에 비밀번호를 넣으면 저장장치의 내용을 읽을 수 있다.

이 저장장치는 Tails 전용으로 쓰도록 하자. Ext4는 Linux 전용 파일 시스템이기 때문에, Windows로 부팅한 상태에서는 (별도 프로그램을 사용하지 않는 한) 파티션을 읽을 수 없다. Tails를 포함한 Linux에서는 바로, Windows와 macOS에서는 별도 프로그램을 설치하여 Ext4로 포맷된 파티션을 사용하는 것이 가능하기는 하나 추천하지는 않는다. 캐시 데이터가 운영체제 파티션에 남을 수 있고, Windows/macOS에서는 불안정하다. Tails용으로 세팅한 저장장치는 Tails에서만 사용하는 것이 바람직하다.

7. Windows/macOS와 병용

Tails 공식 홈페이지 PC에서 Tails 시작하기 페이지
Tails 공식 홈페이지 Mac에서 Tails 시작하기 페이지
Windows로 부팅하고 싶을 때에는 Tails 부트 미디어를 뺀 상태로 컴퓨터를 켜면 된다. Tails로 들어가고 싶을 때에는 처음 설치할 때 했던 것처럼 Tails 부트 미디어를 삽입하고 컴퓨터를 켠 후, Tails 부트 미디어로 부팅하면 된다.

Apple 기기(Mac, MacBook 등)는 부팅할 때 키보드 option(Alt) 키를 누르고 있으면 부팅 메뉴가 뜬다. Apple 기기는 희한하게도 부팅 디스크 고르는 창에서 Tails를 선택하면 컴퓨터가 작동을 멈춰 버리는(얼어 버리는) 경우가 있다. 이럴 땐 전원 버튼을 길게 눌러 강제 종료한 후 다시 시도하면 된다. 다시 시도해도 역시나 얼어 버리는 경우가 있는데, 강제 종료 후 재시동을 반복하면 언젠가는 부팅이 된다. 상식과는 달리, 전원 버튼을 눌러 컴퓨터를 강제 종료한다고 컴퓨터 부품에 무리가 가거나 하지는 않으니 계속 반복적으로 이렇게 해도 된다.

8. 인터넷 이용

Tails 공식 홈페이지 Unsafe Browser 페이지
Tails에는 Tor 브라우저, Unsafe Browser 총 2가지 브라우저가 기본 탑재되어 있다. Tor 브라우저를 사용해야 한다. Unsafe Browser를 사용하면 IP 우회 없이 인터넷에 연결되며, #시작 화면(Welcome Screen) 문단에서 서술했듯 인터넷을 이용하라고 넣은 기능이 아니다. 왜 Unsafe Browser를 비활성화할 수 있도록 조치했겠는가.

한편, Tails와 VPN을 함께 사용하여 Unsafe Browser로 VPN을 통해 웹서핑을 하면 좋지 않겠냐고 생각하는 사람도 있을 수 있다. Tor는 속도가 느려서 답답하니까 속도가 빠른 VPN을 사용하겠다는 것이다. 나쁜 방법은 아니다. 하지만 앞서 언급한 바와 같이 Tails는 한 번 껐다 켤 때마다 모든 설정이 초기화되므로 이걸 하려면 OpenVPN 클라이언트 설치를 비롯해 VPN 세팅도 매번 다시 해 줘야 한다.[4] 그리고 당연하게도 Tor 브라우저를 쓸 때보다 익명성이 현저히 떨어지는 것은 감수해야 한다. 세 가지 측면에서 그렇다.

1. 접속하는 사이트(목적지) 입장에서 봤을 때 더 눈에 띄는 유저가 된다. Tor 브라우저의 익명성은, 웹사이트 입장에서 봤을 때 모든 Tor 브라우저 이용자들이 다 똑같아 보이게 함으로써 달성되는 것이다. Unsafe Browser를 가지고 VPN IP를 통해 접속하는 것은 이와 같은 '똑같아 보이는 성질'을 포기하는 것이다.
2. ISP 입장에서는 내가 어떤 사이트에 방문하는지를 알아내기가 더 쉬워진다. 앞서 언급한 Website Fingerprinting 이슈다.
3. 나의 실제 신상정보와 내가 방문하는 사이트 정보를 동시에 아는 사람이 존재하게 된다. Tor를 사용하면 노드(중간 경유지) 세 단계를 기본적으로 거치기 때문에 나의 신상정보 및 내가 어떤 사이트에 방문하고 있는지에 관한 정보를 동시에 아는 사람은 거의 존재하지 않게 된다. 하지만 VPN을 사용하면 '내 컴퓨터 - VPN - 목적지' 식으로 노드가 구축되므로 VPN 회사는 내가 어떤 사이트에 방문하는지를 손쉽게 알 수 있다. 설령 VPN 회사가 no-logs policy를 철저하게 지킨다 해도, VPN 회사가 사용하는 데이터센터와 ISP는 당연히 로그를 보유하고 있다. 생각해 보자. 내가 내 컴퓨터에서 브라우징 히스토리를 완전히 삭제한다 해도, 내가 사용하는 ISP는 여전히 그 브라우징 히스토리를 보유하고 있지 않는가? VPN도 마찬가지다.

ISP는 내 실제 IP와 내가 접속하는 사이트의 IP(및 도메인[5])을 동시에 로그로 남길 수 있다. 실제로 경찰은 no-logs policy로 운영되는 EarthVPN 이용자를, EarthVPN 서버가 위치한 데이터센터의 로그를 확보함으로써 추적해 낸 바 있다. 따라서, Unsafe Browser와 VPN을 병용하는 것보다 Tor 브라우저를 사용하는 것이 낫다. Unsafe Browser는 그러라고 내장되어 있는 것이 아님을 재차 언급한다.

다만 **중국(홍콩/마카오 포함) 내에서 Tor 브라우저를 사용하는 경우 Tails 사용을 재고할 필요**가 있다. 중국 정부는 황금방패 등 **자국 인터넷 검열을 회피하려는 시도 그 자체를 불법으로 규정**한다. 물론 성인 사이트 정도는 외국인이라면 가볍게는 구두 경고에서 심해봐야 강제 추방이나 재입국 금지 정도로 끝날 가능성이 높지만. 애초에 외국인 전용 회선 같은 경우엔 검열을 풀어주기도 한다. 동네 카페 Wi-Fi, PC방 등 중국 현지인도 같이 쓰는 회선이나 컴퓨터에서 쓰게 되면 공안이 찾아올 수도 있다는 거다.

Persistence Storage를 설정할 때 북마크 부분에도 체크를 해 두었다면, Tor 브라우저 북마크(즐겨찾기)는 Tails를 종료해도 그대로 남는다. 필요한 경우 이 기능을 이용하자.

양파 아이콘에서 Security Settings를 눌러 보면 Security Slider라는 것이 나와서 보안 레벨을 3단계로 설정할 수 있다. Default는 가장 낮은 레벨이다. 높은 레벨로 설정해 놓으면 JavaScript를 차단하기 때문에 보안성은 높아지지만 그 반대급부로 제대로 작동을 안 하는 사이트가 늘어난다. 웹사이트의 원활한 동작을 위해서는 Default를 권장한다.

Tor 네트워크 속도가 느리다면 양파 아이콘에서 New Tor circuit for this site를 클릭하여 노드를 바꿔 보자. 속도가 느린 노드가 걸리면 느려지고, 속도가 빠른 노드가 걸리면 빨라진다. 수 년 전에 비해 Tor 네트워크의 속도가 많이 빨라졌다.
이게 뭘 시사하는지 생각해 볼 필요가 있다. 네트워크 속도가 빨라졌다는 것은 넓은 대역폭을 갖춘 노드(서버)가 많아졌다는 뜻이다. 그런 노드를 지속적으로 운영하려면 많은 돈이 든다. 그 돈이 다 어디서 나왔을까? Tor 이용자를 감시하고자 하는 국가기관들이 배후에 있을 가능성이 있다. **Tor 브라우저로도 아동 포르노그래피 시청은 하지 마라. Tor를 사용하는 것만으로는 결코 국가기관보다 우위를 점할 수 없다.**

'어떤 ISP를 이용하는지' 및 '접속 시간대'도 Tor 속도에 영향을 준다. 알 사람은 다 아는 사실이지만, kt는 해외망이 잘 돼 있어서 해외 접속이 빠른 반면, SK브로드밴드는 해외망이 부실해서 해외 접속이 느리다[6]. 낮에는 해외망이 부실한 ISP를 쓰더라도 체감이 잘 안 되지만, 수많은 사람들이 해외망으로 몰리는 저녁 시간대가 되면 크게 체감된다. 그런데 Tor 네트워크에 접속하려면 당연하게도 해외망을 거쳐야 하므로 Tor 네트워크보다도 ISP 해외망 속도가 느린 경우 ISP가 병목(bottleneck)으로 작용하여 Tor 속도가 느려진다. 사실 Tor 사용자는 대부분 미국이나 유럽 등 서구권 사람들이고, Tor 노드도 대부분 서구권 국가에 위치한다. 아직까지는 우리나라를 포함한 동아시아 국가들에는 Tor를 쓰는 사람이 그리 많지 않다. 그럼에도 우리나라에서 아침이나 낮(미국은 저녁)에는 Tor가 빠르고 우리나라에서 저녁(미국은 오전)에는 Tor가 느린 이유가 무엇이겠는가? 해외망 때문이다.
이 문제를 해결하려면

1. Tails를 재부팅하여 Tor 노드를 바꾸어 보거나[7]
2. 아침~오후 시간대에 접속하거나[8]
3. ISP를 kt로 바꾸거나[9]
4. 집이 아닌 다른 곳(가령 모텔[10])에서 Tor 접속을 시도하는 방법이 있다.

ISP 해외망이 부실한 경우, 요금제를 업그레이드한다고 해서 저녁 시간대 해외망 속도가 빨라지지 않는다. 국내망 속도만 빨라질 뿐이다.

구글 CAPTCHA를 이용하는 사이트에 Tor 브라우저로 접속하면, 아예 문제를 풀 기회도 주지 않고 그냥 접속을 차단해

버리는 경우가 있다. 그럴 땐 New Tor circuit for this site를 눌러서 다시 시도하면 된다. 사이트마다 다르지만, 아주 여러 번 시도해야 하는 경우도 있다.

Tails 내 Tor 브라우저가 접근 가능한 디렉터리는 단 2개, 전원을 끄면 삭제되는 amnesia/Tor Browser와 Persistence Storage 내 Tor Browser 디렉터리뿐이다. 일단 다운로드가 완료된 후에는 탐색기에서 아무 폴더로나 자유롭게 이동, 복사 가능하고, 파일을 업로드하려면 먼저 이 디렉터리로 옮겨 작업해야 한다.

8.1. Tor 브릿지 접속 불가 문제 해결

2023년 12월 현재 이 문제는 해결됐다. Tor 네트워크에 연결할 때 자동으로 시간대가 바뀌어서 아무 문제 없이 브릿지 접속이 된다. 그럼에도 문제를 겪을 경우를 대비하여 이 문단은 삭제하지 않고 남겨둔다.
🔗 관련 글 1, 🔗 관련 글 2, 🔗 관련 글 3

브릿지 연결이 잘 안 될 수 있다. Tor 네트워크 연결에는 시간 동기화가 필요하며, 현재 시각이 정확히 설정되어 있는 경우가 대부분이므로 많은 경우 Windows/Linux 간 시간대 처리 방식이 달라 이 문제가 발생한다.[11] 이를 해결하기 위해서는 레지스트리 수정이 필요하다. 하단 명령어를 실행하여 빠르게 해결하자. 명령 프롬프트 등을 이용해 실행하면 되고, 관리자 권한이 필요하다.

```
reg add "HKEY_LOCAL_MACHINESYSTEMCurrentControlSetControlTimeZoneInformation" /v RealTimeIsUniversal /d 1 /t REG_QWORD /f
```

명령어 실행 후 시간대를 런던(UTC +0)으로 맞추면 대부분 문제가 해결될 것이다.

8.2. 무선 인터넷 연결 문제 해결

🔗 Tails 공식 홈페이지 Wi-Fi 작동 문제 해결 페이지

0. Tails는 인터넷 연결 방식으로 이더넷(유선 연결) 사용을 권장한다.
1. 일부 무선 랜 카드는 호환성 문제로 사용할 수 없다. #하드웨어 호환성 문제 문단에서 목록 확인이 가능하다.
2. 무선 랜 카드를 인식하지 못해 Wi-Fi 작동이 되지 않을 수 있다. 익명성 하락을 감수하고 Welcome Screen에서 MAC 주소 익명화 비활성화를 선택할 경우 이 문제가 해결될 수 있다.
3. 버튼을 눌러야 하는 공공 Wi-Fi 접속에는 Tor 브라우저를 사용할 수 없다. Unsafe Browser를 사용하면 접속 가능하다.
4. 하드웨어 문제가 있는 경우, USB 무선 랜 카드 구입이 가장 빠른 해결책이다. 하드웨어 호환성 문제 문단을 참고하여 호환되는 제품을 구입하자.

9. 익명으로 회원가입하기

일부 사이트는 '실명으로' 회원가입을 하기는 조금 꺼려지는 것이 사실이다. 할 수만 있다면 누구나 익명으로 가입하고 싶을 것이다. 그런데 생각을 해 보자. 꼭 '정식으로' 실명인증 절차를 거치지 않더라도, 내가 항상 쓰는 아이디, 항상 쓰는 비밀번호, 항상 쓰는 이메일을 이용해 회원가입을 하면 그게 곧 실명으로 가입하는 거나 마찬가지가 아니겠는가? 가령 내 아이디와 이메일을 아는 친구가 장난 삼아 유명 성인 사이트에 들어가 '비밀번호 찾기'에서 그 아이디와 이메일을 입력한다고 해 보자. '해당 이메일 주소와 일치하는 회원이 없습니다'라는 메시지가 뜨는 대신, '해당 이메일 주소로 임시 비밀번호가 발급되었습니다' 같은 메시지가 뜬다면, 내가 그 사이트에 가입했다는 사실이 친구에게 걸린 것이다.[12] 웹사이트 정보 유출로 개인정보가 유포된 경우, 이메일 주소와 ID를 바탕으로 가입 여부를 특정할 수 있다.

실명인증을 하지 않더라도, 내가 항상 쓰는 아이디와 비밀번호와 이메일 주소 등으로 가입한다면 그건 실질적으로 실명 가입이나 마찬가지다.

아래에서는 익명으로 회원가입하는 방법에 대해 알아본다. 이렇게 한다고 완벽한 익명성이 보장되는 것은 전혀 아니지만 후술할 조치를 아예 안 하는 것보다는 낫다.

9.1. 이메일 인증이 불필요한 경우

0. 우선, 이메일 인증 없이 아이디와 비밀번호만으로 회원가입이 완료되는 사이트(예를 들어 Xvideos, xHamster 등)에 가입한다고 가정해 보자. 아이디와 비밀번호를 지금까지 쓰던 것과 완전히 다르게 만들면서도 그걸 일일이 기억하려면 부담스럽다. 다행히 Tails에는 KeePass와 유사한 Linux용 비밀번호 관리자 프로그램인 KeePassX가 기본으로 탑재되어 있다.
1. Applications → KeePassX (이하 '키패스')를 실행시켜 보자. 키패스 메뉴에서 Database → New database를 눌러 새로운 데이터베이스 파일을 만든다. 데이터베이스 비밀번호를 설정하는 창이 뜨는데, 앞으로 이 데이터베이스에 저장할 아이디/비밀번호 내역들이 지금 설정하는 데이터베이스 비밀번호로 암호화된다고 생각하면 된다. 이 데이터베이스 파일을 어디 드랍박스 같은 데 올릴 계획이 아니라면, 그리고 Persistence Storage 비밀번호를 강력하게 설정했다면 지금 이 데이터베이스 비밀번호는 굳이 강력하게 만들 필요가 없다. 그냥 1234 정도로 지정해도 충분하다. 어차피 Persistence Storage에 저장되는 모든 파일은 LUKS로 암호화되기 때문이다.
2. 비밀번호를 설정했으면, Database → Save database를 눌러 방금 만든 데이터베이스를 파일 형태로 저장하되, Persistence Storage 폴더 안에 저장한다(Persistence Storage 밖에 저장하면 Tails를 종료하는 순간 파일이 삭제된다). 파일 이름은 아무렇게나 해도 상관없지만, 편의상 keepassx.kdbx라고 저장하면 좋다.
3. 이제 Entries → Add new entry를 누른다. (나중에 실제로 키패스를 사용할 땐 이렇게 일일이 메뉴를 들어가서 누르기보다는 금색 열쇠모양 아이콘이나 Ctrl + N이라는 단축키를 더 자주 사용하게 될 테지만, 여기에서는 설명의 편의상 그냥 메뉴를 가지고 설명한다.) Title에는 가입할 사이트의 이름을, Username에는 그 사이트의 아이디를, Password에는 그 사이트의 비밀번호를, Repeat에는 똑같은 비밀번호를, URL에는 그 사이트의 주소를 적으면 된다. 지금은 시험 삼아 그냥 각각의 항목에 키보드로 아무거나 입력하고 OK를 눌러 보자. 그러면 방금 만든 entry가 리스트에 추가돼 있는 모습을 볼 수 있을 것이다.
4. 이제 변경 내용을 저장하고 프로그램을 닫을 차례다. 창을 닫기 전에, Tools → Settings로 들어가 Automatically save after every change에 체크가 돼 있는지 확인해 보자. 만약 거기에 체크가 돼 있다면 변경내용은 이미 자동으로 저장되어 있으므로 따로 뭘 할 필요 없이 창을 닫아도 상관없다. 만약 체크가 되어 있지 않다면, 수동으로 체크를 해 주고 Ctrl + S를 눌러 저장을 하고 창을 닫으면 된다.
5. 한편, 키패스에는 '비밀번호 생성기'라는 유용한 기능이 있다. (꼭 키패스가 아니라도 비밀번호 관리 프로그램이라면 다들 갖추고 있는 기능이다.) Entries → Add new entry를 눌러 보자. Repeat 항목 옆에 Gen.이라는 버튼이 보일 것이다. 그걸 누르면 랜덤한 비밀번호가 하나 생성된다. Exclude look-alike characters 및 Ensure that the password contains characters from every group 항목은 특별한 사정이 없는 한 체크하지 '않는' 것이 좋다. 그래야 더 강력한 비밀번호가 생성된다. '이 비밀번호를 어떻게 키보드로 치나' 하는 걱정은 하지 않아도 좋다. 어차피 복붙으로 입력할 것이다. 생성된 비밀번호가 마음에 들면 아래에 있는 Accept 버튼을 누르면 된다.
6. 키패스 프로그램 사용법을 다 익혔으니 이제 실제 회원가입 상황을 상정해 보자. 우선 아이디를 정해야 할 텐데, 아이디도 직접 정하는 것보다는 방금 말한 비밀번호 생성기를 이용해서 랜덤하게 생성하는 것이 더 간편하고 좋다. 아이디에는 특수문자를 허용하지 않는 사이트들이 많으므로, Character types에서 A-Z, a-z, 0-9만 선택하고 /*-_...는 선택하지 않은 상태로 적당한 길이의 문자열이 생성되도록 한 후, 그 문자열을 복사해서 위 Username 부분에 붙여넣기 한다. 아이디를 정했으니 이제는 비밀번호를 정할 차례다. 사이트마다 비밀번호 글자수 제한이 다른데, 웬만하면 사이트가 허용하는 한도 내에서 최대한 길게 만드는 것이 좋다. 12자 제한인 곳이라면 12자, 20자 제한인 곳이면 20자로 만드는 식으로. 무제한인 곳이라면 한 16자 정도로 하면 무난할 듯하다. 겉으로는 무제한인 것처럼 보이지만 실제로는 유저 몰래 16자 제한을 걸어 둔 곳이 많아서 그렇다. 비밀번호도 정했으면 Title과 URL을 입력하고 OK를 눌러 저장한다.
7. 이제 가입하고자 하는 사이트의 회원가입 페이지로 들어가 본다. 요즘은 회원가입 페이지에 구글 캡챠 (I'm not a robot에 체크하고 그림문제 푸는 것)를 걸어 놓은 사이트가 많다. 아이디/비밀번호를 치기 전에 캡챠 먼저 푸는 것을 추천한다. 만약 구글이 캡챠를 풀 기회도 주지 않고 차단해 버리면 New Tor circuit for this site 버튼을 누르고

다시 시도해 본다. 캡챠를 풀었으면 Entries → Copy username을 누른 후 사이트의 '아이디' 부분에 붙여넣기하고, Entries → Copy password을 누른 후 사이트의 '비밀번호' 부분에 붙여넣기하여 회원가입을 완료한다.

8. 나중에 로그인할 때에도 같은 방법으로 아이디, 비밀번호를 복붙하면 된다. 그런데 간혹 회원가입시 설정한 아이디, 비밀번호를 정확히 복붙했는데도 '비밀번호가 틀렸습니다'라는 메시지가 나오는 경우가 있다. 이 문제는 주로 그 사이트에 비밀번호 글자수 제한이 '숨겨져' 있었던 경우에 발생한다. 회원가입할 때 키패스로 한 30자리 비밀번호를 만들어서 입력할 땐 아무런 에러 메시지도 뜨지 않고 정상적으로 회원가입이 완료됐지만, 실제로는 사이트가 유저 모르게 그 30자리 중 맨 앞 16자리까지만 비밀번호로 삼고 뒤에 있는 나머지 14자리는 그냥 짤라 버린 경우이다. 이 경우 키패스에 저장돼 있는 30자리 비밀번호 중 앞 16자리만 복붙해서 로그인을 시도하면 정상적으로 로그인이 된다. 문제는 이 사이트가 앞 16자리를 사용했는지 12자리를 사용했는지 20자리를 사용했는지 어디 정확히 나와 있는 데가 없다는 것이다. 보통 16, 20, 12인 경우가 많으니 차례로 시도해 보자. 그래도 안 되면 '비밀번호 찾기'를 하거나, 12자 정도의 짧은 비밀번호로 재가입해 보자.
9. KeePassX의 랜덤 패스워드 생성 기능을 사용하면 실수로 익명성이 깨질 위험을 낮출 수 있다. Tor 브라우저를 이용해 익명으로 회원가입을 하면서 본인이 머리로 직접 만들어낸 아이디와 비밀번호를 사용하는 경우, Tor 브라우저를 사용하지 않는 '익명성이 깨진 상태'에서 그 사이트에 그 아이디와 비밀번호로 로그인하는 것이 가능해진다. 한 번이라도 그렇게 로그인하는 순간 익명성은 깨진다. 지금까지 그 아이디로 한 모든 활동 내역이 이제 실명 상태인 나에게 귀속되는 것이다. 반면, 랜덤 아이디/비밀번호를 만들어서 KeyPassX에만 저장해 놓고 항상 복사-붙여넣기로만 로그인하는 경우에는 그런 실수를 할 가능성이 아예 없어진다.

9.2. 이메일 인증이 필요한 경우

0. 회원가입 시 이메일 인증을 요구하는 사이트에 익명으로 회원가입을 하려면 먼저 새로운 이메일 주소부터 만들어야 한다. 그런데 익명으로 회원가입을 받아주는 이메일 서비스는 생각보다 찾기 힘들다. 네이버나 다음 등 국내 서비스는 물론 Gmail과 야후! 메일도 가입할 때 휴대폰 인증, 최소한 다른 이메일 주소를 인증할 것을 요구한다. 두 가지 방법으로 대처할 수 있다.

1. Gmail 등의 상용 이메일 서비스에 실명으로 새로 가입하는 방법이 있다. 예를 들어 Gmail에서 휴대폰 인증을 거쳐 asdzxc556@gmail.com이라는 메일주소를 새로 만들었다고 하자. 이때, 그 메일주소가 '나'의 것이라는 사실을 아는 사람은 구글뿐이다. 가족이나 친구도 모르고, 그 이메일 주소로 가입을 받아 준 사이트도 모른다. 이동통신사는 구글에서 보낸 인증코드 문자내역을 들여다볼 수 있으므로 내가 그 시점에 Gmail에서 새로운 메일계정을 하나 만들었다는 사실을 알지만, 내가 만든 계정이 정확히 'asdzxc556'이라는 사실은 모른다.
2. 익명으로 가입을 받아 주는 무료 이메일 서비스를 찾아내어 사용할 수도 있다. 익명으로 사용할 수 있는 임시 이메일을 발급해 주는 곳으로는 Guerrilla Mail, Mailinator, Email On Deck 정도를 꼽을 수 있다. 정식으로 장기간 사용할 만한 메일은 아니지만, 회원가입시 이메일 인증메일 1개 정도를 받는 용도로는 적합하다. 게릴라메일이나 메일리네이터는 워낙 유명한 서비스라 그 메일주소를 입력하면 가입을 거절하는 사이트들이 많다. 이메일온덱은 게릴라메일이나 메일리네이터에 비해 가입을 거절당할 확률이 훨씬 낮다. 되도록이면 이메일온덱을 이용하는 것이 좋다.
   원래 임시 이메일로 쓰라고 나온 건 아닌데 실질적으로 임시 이메일처럼 쓸 수 있는 서비스로는 Countermail이 있다. 캡차만 풀면 익명으로 회원가입 가능하며, 체험판 명목으로 무료로 7일 동안 사용할 수 있다. 계속 사용하려면 유료결제를 해야 한다.
3. 만약 익명으로 무료로 가입할 수 있으면서도 Gmail처럼 장기간 안정적으로 사용할 수 있는 이메일을 찾는다면 Tutanota[13], Disroot.org, 오픈메일박스, Onionmail, 아웃룩[14]이 좋다. 가입 과정에서 구글 캡챠를 풀어야 하기는 하지만, 그 밖에 다른 이메일 주소 인증이나 휴대폰 번호 인증을 요구하지는 않는다. Tor 브라우저만 가지고 순수하게 익명으로 가입이 가능하다. 물론 여기에 가입할 때 사용하는 아이디/비밀번호는 평소 쓰던 것과 전혀 다르게 만들어야 하며, KeePassX에 등록해 놓음으로써 까먹지 않도록 해야 한다.
4. ProtonMail은 익명으로 가입하려면 좀 복잡하다. 그냥 생 아이피를 노출시키면서 가입을 시도하거나, Tor 브라우저가 아닌 일반 VPN을 이용해서 가입을 시도하면 따로 개인정보를 제공하지 않고 구글 캡챠만 풀어도 쉽게 가입이 가능하다. 하지만 생 아이피를 그대로 노출시키면서 가입하는 것은 물론, VPN을 이용해서 가입하는 것도 익명 가입이라고 할 수 없다.[15] Tor 브라우저로 접속해서 가입을 시도하면 운 나쁜 경우에는 휴대폰 인증 또는 신용카드 인증만 가능하고(당연히 익명성이 약화된다), 운 좋은 경우에는 이메일 인증도 가능하다. 이메일 인증이 열려 있는 경우에는 익명으로 가입할 수 있다. ProtonMail이 아닌 다른 서비스에서 익명으로 이메일 주소를 하나 만들고, 그 이메일 주소를 ProtonMail 가입용으로 활용하면 된다.
5. LTE 등 이동통신사 무선망(통신사 IP)으로 회원가입을 시도하진 말자. 실명 회선을 통해 할당된 IP로 인터넷에 접속하는 것이므로, 로그 대조를 통해 추적 가능하다. 이동통신사와 경찰 간 공조가 되어야 가능하지만 익명성이 깨지는 것은 분명하다.
6. 익명성 유지와 관련해서 유의할 점이 하나 있다. 만약 사이트1에서 활동하는 사람과 사이트2에서 활동하는 사람이 동일인이라는 사실을 남들에게 노출시키고 싶지 않다면, ID/비밀번호를 모두 다르게 설정하는 것은 기본이요 가입할 때 기입하는 이메일 주소도 달라야 한다. 이메일 서비스에 익명으로 2번 가입해야 하는 것이다.

10. 비트토렌트 사용?

Tails로 비트토렌트 사용은 권장되지 않는다. Tor 망에서 토렌트 사용은 상당한 민폐고, 그런다고 해서 익명성이 확실하게 보장되는 것도 아니다.[16] 토렌트를 이용하려면 다른 방법을 찾는 것이 좋다. 개인적으로는 스트리밍 또는 직접 다운로드를 추천한다. 굳이 토렌트를 사용해야만 한다면, Tribler 등 IP 우회를 지원하는 클라이언트를 안전한 VPN 서비스와 병행 사용하는 것을 권장한다.

11. Tails 업그레이드

Tails 공식 홈페이지 업그레이드 페이지
Tails 공식 홈페이지 소식 페이지
Tails는 업데이트를 업그레이드라고 부른다.

Tails에는 자동 업그레이드 시스템이 내장되어 있다. 마이너 릴리즈[17]와 패치 릴리즈[18]는 네트워크에 연결되어 있을 때 자동으로 확인되고, 설치할 수 있다.
Tails 업그레이드에는 버그 수정, 보안 취약점 수정, 내장 소프트웨어 업데이트가 포함되어 있으므로 기회가 되는 대로 업그레이드를 받는 것을 강력히 권한다. 마이너 업그레이드는 보통 4주에 1회 진행되며, 긴급 보안 패치가 있을 경우 이를 반영한 패치 릴리즈가 나온다.

12. 사용 종료 직후 해야 할 일

Tails 부트 미디어를 제거하지 않고, 버튼을 누르는 방법으로 전원 종료를 했다면 컴퓨터가 완전히 꺼진 후 Tails 부트 미디어를 컴퓨터에서 제거한다.
Tails 부트 미디어가 꽂혀 있는 상태로 다른 운영체제로 부팅하거나, 다른 운영체제로 부팅된 상태에서 Tails 부트 미디어를 삽입하는 상황은 피하는 것이 바람직하다.

13. Tails 부트 미디어 초기화

주의: 이 작업을 수행할 경우 안에 담긴 모든 데이터가 삭제된다.
Tails 부트 미디어를 초기화하고 싶다면 디스크 관리 프로그램을 이용하여야 한다. Windows 기준으로 설명했다. mac OS/Linux 사용자는 각자에게 맞는 방법으로 해결할 수 있으리라 믿는다.

1. 일단 USB를 꼽는다.
2. 윈도우 검색창에 diskpart 입력하고 실행한다.
3. list disk 입력하고 엔터.
4. USB가 disk 0인지 1인지 2인지 확인.
5. 만약 USB가 disk 1 이라면, select disk 1 입력하고 엔터.

6. clean 입력하고 엔터.
7. exit 입력하고 엔터.
8. 윈도우 검색창에 '하드 디스크 파티션 만들기 및 포맷' 입력하고 실행한다.
9. disk 1이 '할당되지 않음' 상태인 것이 보일 것이다. 우클릭하고 '새 단순 볼륨' 클릭한다.
10. '다음'을 쭉 누른다. 단 '이 볼륨을 다음 설정으로 포맷'의 '파일 시스템'을 NTFS에서 FAT32로 바꿔준다. 새로 산 USB를 '하드 디스크 파티션 만들기 및 포맷'에서 확인해 보면 FAT32임을 알 수 있다. 32GB USB는 NTFS와 FAT32가 있는데 64GB 이상부터는 FAT32대신 exFAT가 있다.
11. 나머지 과정을 모두 마친다.

만약 CMD 창 내에게 모든 과정을 마치고 싶고 명령어를 잘 알고 있다면 아래과 같이 하면 된다.

1. Windows로 부팅 후, Tails 부트 미디어를 삽입한다.
2. Windows+S 키를 누르고[19], diskpart를 입력하고 Enter. 필요한 경우 Alt+Y를 눌러 관리자 권한을 부여한다.
3. lis dis 입력 후 Enter.
4. 연결된 모든 드라이브가 확인된다. 나타나는 정보를 바탕으로 Tails 부트 미디어의 디스크 번호를 확인한다.
5. sel dis (번호) 입력 후 Enter.
6. clean 입력 후 Enter.
7. con mbr 입력 후 Enter.
8. cre par pri 입력 후 Enter.
9. for quick 입력 후 Enter.
10. exit 입력 후 Enter.

모든 작업을 수행한 후 파일 탐색기를 열면 USB 드라이브라는 이름으로 포맷된 이동식 저장장치를 확인할 수 있을 것이다.

---

[1] AMD 그래픽 카드는 후술하듯 부팅 옵션 수정이 필요한 경우가 있다. 특히 Radeon HD/RX Vega 시리즈.

[2] 드라이버 소프트웨어 내장

[3] 버튼을 눌러야 접속 가능한 Wi-Fi가 대표적이다.

[4] 단, VPN 클라이언트 공유기에 접속하여 Unsafe Browser를 사용하면 별도 설정 없이 자동으로 VPN을 통해 접속된다.

[5] VPN의 ISP는 목적지 웹사이트의 IP뿐만 아니라 도메인, 즉 주소도 알 수 있다. 설령 그 웹사이트에 HTTPS로 접속한다 해도, 그리고 VPN 회사가 자체 DNS를 운영한다 해도 마찬가지다.

[6] LG U+는 사람마다 평이 갈리는 것 같다

[7] 큰 도움은 되지 않는다. 본질적인 해결책도 아니다.

[8] 이 시간대는 해외망 수요가 비교적 적다.

[9] kt는 ISP 중 해외망 품질이 가장 낫다.

[10] 모텔 객실에는 대부분 컴퓨터가 한두 개씩 있다. 물론 모텔에서 사용하는 ISP가 해외망이 부실하면 돈 날리는 꼴이 되겠지만.

[11] macOS 파일명 한글 자모분리 문제와 유사하다.

[12] 이를 응용한 방법이 2014년 5월 일간베스트저장소 가입 여부 확인법으로 널리 알려진 바 있다.

[13] 계정 생성하는 데 매우 오래 걸리며, Tor 망에서 가입한 경우 계정이 생성은 되지만 스팸 방지 명목으로 사용 불가 처리가 될 수 있다.

[14] Outlook.com은 대기업 이메일로서는 특이하게도 Tor 망에서 가입할 수 있으나, 정책이 수시로 바뀌므로 갑자기 불가능해질 수 있다. 가입이 무사히 되더라도 Tor 망으로 계속 접속하면 보안 문제로 계정이 차단될 수 있다. Tor를 사용하는 경우 접속 위치가 수시로 바뀌므로 계정 탈취로 간주할 수 있다.

[15] VPN은 애초에 (목적지 웹사이트에 대한) 익명성 유지를 위해 만들어진 도구가 아니다.

[16] 비트토렌트 프로토콜은 사용자의 IP가 그대로 노출될 정도로 익명성이 전혀 보장되지 않는 프로토콜이다.

[17] 예 - 5.19에서 5.20

[18] 예 - 5.19의 보안 취약점을 긴급 수정한 5.19.1

[19] 복사를 위해 Ctrl+C를 누르는 것처럼

이 문서의 내용 중 전체 또는 일부는 Tails OS 문서의 r227 판에서 가져왔습니다. 이전 역사 보러 가기

이 저작물은 CC BY-NC-SA 2.0 KR에 따라 이용할 수 있습니다. (단, 라이선스가 명시된 일부 문서 및 삽화 제외)
기여하신 문서의 저작권은 각 기여자에게 있으며, 각 기여자는 기여하신 부분의 저작권을 갖습니다.

나무위키는 백과사전이 아니며 검증되지 않았거나, 편향적이거나, 잘못된 서술이 있을 수 있습니다.
나무위키는 위키위키입니다. 여러분이 직접 문서를 고칠 수 있으며, 다른 사람의 의견을 원할 경우 직접 토론을 발제할 수 있습니다.